Finite Fields and Their Applications **8,** 570–588 (2002)
doi:10.1006/ffta.2002.0365

Compressing Mappings on Primitive Sequences over $Z/(2^e)$ and Its Galois Extension[1]

Qi Wenfeng[2] and Zhu Xuanyong

Department of Applied Mathematics, Zhengzhou Information Engineering University, P.O. Box 1001-745, Zhengzhou, 450002, People's Republic of China
E-mail: wenfeng.qi@263.net,zhuxuanyong@263.net

Communicated by Rudolf Lidl

Received March 11, 2001; revised February 10, 2002; published online June 25, 2002

Let $f(x)$ be a strongly primitive polynomial of degree n over $Z/(2^e)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a Boolean function of $e-1$ variables and

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2})$$

$G(f(x), Z/(2^e))$ denotes the set of all sequences over $Z/(2^e)$ generated by $f(x)$, F_2^∞ the set of all sequences over the binary field F_2, then the compressing mapping

$$\Phi: \begin{cases} G(f(x), Z/(2^e)) \to F_2^\infty, \\ \underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1} 2^{e-1} \mapsto \varphi(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{e-1}) \bmod 2 \end{cases}$$

is injective, that is, for $\underline{a}, \underline{b} \in G(f(x), Z/(2^e))$, $\underline{a} = \underline{b}$ if and only if $\Phi(\underline{a}) = \Phi(\underline{b})$, i.e., $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) = \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$. In the second part of the paper, we generalize the above result over the Galois rings.

Key Words: primitive polynomial; Galois ring; linear sequence; compressing mapping.

1. INTRODUCTION

Let R be a ring, $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ a monic polynomial over R, the sequence $\underline{a} = (a_0, a_1, a_2, \ldots)$ over R satisfying the recursion

$$a_{i+n} = -(c_0 a_i + c_1 a_{i+1} + \cdots + c_{n-1} a_{i+n-1}), \qquad i = 0, 1, 2, \ldots$$

[1]The work is supported by HAIPURT and the Special Fund of National Excellently Doctoral Paper.

[2]To whom correspondence should be addressed.

1071-5797/02 $35.00

is called a linear recurring sequence of degree n over R, generated by $f(x)$. We will use the notation $G(f(x), R)$ for the set of all sequences over R generated by $f(x)$.

Let $\underline{a} = (a_0, a_1, a_2, \ldots)$ and $\underline{b} = (b_0, b_1, b_2, \ldots)$ be sequences over R and $c \in R$, define

$$\underline{a} + \underline{b} = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$

$$c\underline{a} = (ca_0, ca_1, ca_2, \ldots),$$

$$\underline{a}\underline{b} = (a_0 b_0, a_1 b_1, a_2 b_2, \ldots)$$

and the shift operator x of sequence as $x\underline{a} = (a_1, a_2, a_3, \ldots)$ and $x^k\underline{a} = (a_k, a_{k+1}, a_{k+2}, \ldots)$ for $k = 0, 1, 2, \ldots$. Then for any polynomial $f(x)$ over R, $\underline{a} \in G(f(x), R)$ if and only if $f(x)\underline{a} = \underline{0}$.

Let $f(x)$ be a monic polynomial of degree n over $Z/(2^e)$ with $f(0) \not\equiv 0 \bmod 2$, then there exists a positive integer P such that $f(x)$ divides $x^P - 1$ over $Z/(2^e)$. The least such P is called the period of $f(x)$ over $Z/(2^e)$ and denoted by $\mathrm{per}(f(x))$. The period of $f(x)$ is upper bounded by $2^{e-1}(2^n - 1)$, where $n = \deg f(x)$. A monic polynomial $f(x)$ of degree n over $Z/(2^e)$ is called a primitive polynomial if $\mathrm{per}(f(x)) = 2^{e-1}(2^n - 1)$.

Let $f(x)$ be a primitive polynomial of degree n over $Z/(2^e)$, $T = 2^n - 1$, then $f(x) \bmod 2$ is a primitive polynomial over the binary field F_2 and for $i = 1, 2, \ldots, e-1$, we have

$$x^{2^{i-1}T} - 1 \equiv 2^i h_i(x) \bmod f(x), \tag{1}$$

where $h_i(x)$ is a polynomial over $Z/(2^e)$ of degree less than n such that $h_i(x) \not\equiv 0 \bmod 2$. Furthermore,

$$h_2(x) \equiv \cdots \equiv h_{e-1}(x) \bmod 2,$$

$$h_2(x) \equiv h_1(x) + h_1(x)^2 \bmod (2, f(x)). \tag{2}$$

If $e \geq 3$ and $h_2(x) \not\equiv 1 \bmod 2$ or $e = 2$ and $h_1(x) \not\equiv 1 \bmod 2$, then $f(x)$ is called a strongly primitive polynomial over $Z/(2^e)$ (see [1, 3]).

Any element a in $Z/(2^e)$ has a unique binary decomposition as $a = a_0 + a_1 2 + \cdots + a_{e-1}2^{e-1}$, $a_i \in \{0, 1\}$. Similarly, a sequence $\underline{a}$ over $Z/(2^e)$ has a unique binary decomposition as $\underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1}2^{e-1}$, where $\underline{a}_i = (a_{i0}, a_{i1}, a_{i2}, \ldots)$ is a binary sequence over $\{0, 1\}$. The sequence $\underline{a}_i$ is called ith level component of $\underline{a}$, and $\underline{a}_{e-1}$ the highest level component of $\underline{a}$.

There are many papers to discuss the properties of the level component of $\underline{a}$, please refer to [1–5, 7, 8].

In the first part of the paper, we prove the following result. Let $f(x)$ be a strongly primitive polynomial of degree n over $Z/(2^e)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a Boolean function of $e-1$ variables and

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}).$$

F_2^∞ denotes the set of all sequences over the binary field F_2, then the compressing map

$$\Phi: \begin{cases} G(f(x), Z/(2^e)) \to F_2^\infty, \\ \underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1} 2^{e-1} \mapsto \varphi(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{e-1}) \bmod 2 \end{cases}$$

is injective, that is, for $\underline{a}, \underline{b} \in G(f(x), Z/(2^e))$, $\underline{a} = \underline{b}$ if and only if $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$.

In the second part of the paper, we generalize the above result to the one over Galois rings.

2. INJECTIVENESS OF COMPRESSION MAPPINGS OVER $Z/(2^e)$

Huang [3] and Huang and Dai [4] proposed the following injectiveness theorem.

THEOREM 1. *Let $f(x)$ be a primitive polynomial over $Z/(2^e)$, then the mapping*

$$\Phi: \begin{cases} G(f(x), Z/(2^e)) \to F_2^\infty, \\ \underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1} 2^{e-1} \mapsto \underline{a}_{e-1} \end{cases}$$

is injective, that is, for $\underline{a}, \underline{b} \in G(f(x), Z/(2^e))$, $\underline{a} = \underline{b}$ if and only if $\underline{a}_{e-1} = \underline{b}_{e-1}$.

Remark 1. Theorem 1 implies that $\underline{a}_{e-1}$ contains all information of the original sequence $\underline{a}$.

LEMMA 1 (Dai [1]). *Let $f(x)$ be a primitive polynomial of degree n over $Z/(2^e)$, $T = 2^n - 1$, $\underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1} 2^{e-1} \in G(f(x), Z/(2^e))$ and $\underline{a}_0 \neq \underline{0}$, then $\mathrm{per}(\underline{a}_i) = 2^i T$, especially $\mathrm{per}(\underline{a}_{e-1}) = 2^{e-1} T = \mathrm{per}(\underline{a}) = \mathrm{per}(f(x))$.*

LEMMA 2 (Dai [1]). *Let $f(x)$ be a primitive polynomial of degree n over $Z/(2^e)$, $T = 2^n - 1$, $\underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1} 2^{e-1} \in G(f(x), Z/(2^e))$, then $(x^{2^{i-1}T} - 1)\underline{a}_i \equiv h_i(x)\underline{a}_0 \bmod 2$ for $i = 1, 2, \ldots, e-1$. That is, by (2),*

$$(x^{2^{i-1}T} - 1)\underline{a}_i \equiv \begin{cases} h_1(x)\underline{a}_0 \bmod 2 & \text{if } i = 1, \\ h_2(x)\underline{a}_0 \bmod 2 & \text{if } i \geq 2. \end{cases}$$

LEMMA 3. *Let S be a positive integer, $\underline{u}$ a sequence over the ring R with its period dividing S, then for any sequence $\underline{v}$ over R, $(x^S - 1)(\underline{v}\,\underline{u}) = \underline{u}(x^S - 1)\underline{v}$.*

The proof is easy.

LEMMA 4. *Let $f(x)$ be a primitive polynomial of degree n over the finite field F_{2^r}, and $\underline{a} = (a_0, a_1, \ldots)$, $\underline{b} = (b_0, b_1, \ldots)$, $\underline{c} = (c_0, c_1, \ldots) \in G(f(x), F_{2^r})$. If $\underline{a}$, $\underline{b}$ and $\underline{c}$ are linear independent over F_{2^r}, then the number of zeros in $\{a_0b_0, a_1b_1, \ldots, a_{T-1}b_{T-1}\}$ is smaller than the one in $\{a_0b_0c_0, a_1b_1c_1, \ldots, a_{T-1}b_{T-1}c_{T-1}\}$, where $T = 2^{nr} - 1$. Thus $\underline{a}\,\underline{b} \neq \underline{a}\,\underline{b}\,\underline{c}$.*

The proof is easy.

LEMMA 5. *Let $f(x)$ be a primitive polynomial of degree n over $Z/(2^e)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a Boolean function of $e - 1$ variables and*

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}).$$

If $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$ for $\underline{a}, \underline{b} \in G(f(x), Z/(2^e))$, then $\underline{a}_0 = \underline{b}_0$.

Proof. Set $T = 2^n - 1$. The periods of $\eta(\underline{a}_0, \ldots, \underline{a}_{e-2})$ and $\eta(\underline{b}_0, \ldots, \underline{b}_{e-2})$ divide $2^{e-2}T$, so, by $x^{2^{e-2}T} - 1$ acting on $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$, we get

$$(x^{2^{e-2}T} - 1)\underline{a}_{e-1} \equiv (x^{2^{e-2}T} - 1)\underline{b}_{e-1} \bmod 2.$$

Since $\mathrm{per}(\underline{a}_i) = 2^i T$ for $0 \leq i \leq e - 2$, by $x^{2e-2T} - 1 \equiv 2^{e-1}h_{e-1}(x) \bmod f(x)$ acting on $\underline{a}$ and $\underline{b}$, respectively, we have

$$(x^{2^{e-2}T} - 1)\underline{a}_{e-1} \cdot 2^{e-1} = 2^{e-1}h_{e-1}(x)\underline{a}_0,$$

$$(x^{2^{e-2}T} - 1)\underline{b}_{e-1} \cdot 2^{e-1} = 2^{e-1}h_{e-1}(x)\underline{b}_0,$$

that is,

$$(x^{2^{e-2}T} - 1)\underline{a}_{e-1} \equiv h_{e-1}(x)\underline{a}_0 \bmod 2,$$

$$(x^{2^{e-2}T} - 1)\underline{b}_{e-1} \equiv h_{e-1}(x)\underline{b}_0 \bmod 2.$$

So $h_{e-1}(x)\underline{a}_0 \equiv h_{e-1}(x)\underline{b}_0 \bmod 2$. Since $h_{e-1}(x) \not\equiv 0 \bmod (2, f(x))$, we have $\underline{a}_0 = \underline{b}_0$. ■

THEOREM 2. *Let $f(x)$ be a strongly primitive polynomial of degree n over $Z/(2^e)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a Boolean function of $e - 1$ variables and*

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}),$$

then the compressing map

$$\Phi: \begin{cases} G(f(x), Z/(2^e)) \to F_2^{\infty}, \\ \underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1} 2^{e-1} \mapsto \varphi(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{e-1}) \bmod 2 \end{cases}$$

is injective, that is, for $\underline{a}, \underline{b} \in G(f(x), Z/(2^e))$, $a = b$ *if and only if* $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$.

Proof. Let $\underline{a}, \underline{b} \in G(f(x), Z/(2^e))$ with $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$ we shall prove $\underline{a} = \underline{b}$. Since $h_2(x) \equiv \cdots \equiv h_{e-1}(x) \bmod 2$, we set $h(x) = h_2(x) \bmod 2$ which is a polynomial over the field F_2.

Since $\underline{a}_0 = \underline{b}_0$ by Lemma 5, it suffices to consider the case $\underline{a}_0 = \underline{b}_0 \neq \underline{0}$. Set $\eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) = \eta(x_0, x_1, \ldots, x_{e-2})$, then

$$\eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) = x_{e-2}\eta_{e-3}(x_0, x_1, \ldots, x_{e-3}) + \psi_{e-3}(x_0, x_1, \ldots, x_{e-3}).$$

In general, we have

$$\eta_i(x_0, x_1, \ldots, x_i) = x_i \eta_{i-1}(x_0, x_1, \ldots, x_{i-1}) + \psi_{i-1}(x_0, x_1, \ldots, x_{i-1}), \tag{3}$$

where $\eta_{i-1}(x_0, x_1, \ldots, x_{i-1})$ and $\psi_{i-1}(x_0, x_1, \ldots, x_{i-1})$ are Boolean functions with i variables, $i = 1, 2, \ldots, e-1$.

Firstly, we consider the case $e \geq 4$. Since

$$\begin{aligned} &\underline{a}_{e-1} + \underline{a}_{e-2}\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) + \psi_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) \\ &\equiv \underline{b}_{e-1} + \underline{b}_{e-2}\eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3}) + \psi_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3}) \bmod 2 \end{aligned}$$

and the periods of $\psi_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3})$ and $\psi_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})$ divide $2^{e-3}T$, it follows

$$(x^{2^{e-3}T} - 1)\psi_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) \equiv \underline{0} \bmod 2,$$

$$(x^{2^{e-3}T} - 1)\psi_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3}) \equiv \underline{0} \bmod 2$$

and

$$\begin{aligned} &(x^{2^{e-3}T} - 1)(\underline{a}_{e-1} + \underline{a}_{e-2}\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3})) \\ &\equiv (x^{2^{e-3}T} - 1)(\underline{b}_{e-1} + \underline{b}_{e-2}\eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})) \bmod 2. \end{aligned} \tag{4}$$

The periods of $\eta_{e-3}(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{e-3})$ and $\eta_{e-3}(\underline{b}_0, \underline{b}_1, \ldots, \underline{b}_{e-3})$ divide $2^{e-3}T$ and $(x^{2^{e-3}T} - 1)\underline{a}_{e-2} \equiv h(x)\underline{a}_0 \equiv h(x)\underline{b}_0 \equiv (x^{2^{e-3}T} - 1)\underline{b}_{e-2} \bmod 2$, so (4)

implies

$$(x^{2^{e-3}T} - 1)\underline{a}_{e-1} + \eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3})h(x)\underline{a}_0$$
$$\equiv (x^{2^{e-3}T} - 1)\underline{b}_{e-1} + \eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})h(x)\underline{a}_0 \bmod 2,$$

that is,

$$(x^{2^{e-3}T} - 1)(\underline{a}_{e-1} + \underline{b}_{e-1})$$
$$\equiv [\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) + \eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})]h(x)\underline{a}_0 \bmod 2. \tag{5}$$

On the other hand, by $x^{2^{e-3}T} - 1 \equiv 2^{e-2}h_{e-2}(x) \bmod f(x)$ acting on $\underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1}2^{e-1}$, we get

$$(x^{2^{e-3}T} - 1)(\underline{a}_{e-2} + \underline{a}_{e-1}2)2^{e-2} \equiv 2^{e-2}h_{e-2}(x)(\underline{a}_0 + \underline{a}_1 2),$$

that is,

$$(x^{2^{e-3}T} - 1)(\underline{a}_{e-2} + \underline{a}_{e-1}2) \equiv h_{e-2}(x)(\underline{a}_0 + \underline{a}_1 2) \bmod 2^2. \tag{6}$$

Let $h_{e-2}(x)(\underline{a}_0 + \underline{a}_1 2) \equiv \underline{u} + \underline{v}2 \bmod 2^2$, where $\underline{u}$ and $\underline{v}$ are the 0th and 1th level components of $h_{e-2}(x)(\underline{a}_0 + \underline{a}_1 2)$, respectively, then $\underline{u} \equiv h(x)\underline{a}_0 \bmod 2$. By (6),

$$x^{2^{e-3}T}\underline{a}_{e-2} + (x^{2^{e-3}T} - 1)\underline{a}_{e-1}2 \equiv \underline{a}_{e-2} + \underline{u} + \underline{v}2 \bmod 2^2$$

and so

$$(x^{2^{e-3}T} - 1)\underline{a}_{e-1} \equiv \underline{v} + \underline{a}_{e-2} \cdot \underline{u} \bmod 2. \tag{7}$$

Similarly,

$$(x^{2^{e-3}T} - 1)\underline{b}_{e-1} \equiv \underline{w} + \underline{b}_{e-2} \cdot \underline{u} \bmod 2, \tag{8}$$

where $h_{e-2}(x)(\underline{b}_0 + \underline{b}_1 2) \equiv \underline{u} + \underline{w}2 \bmod 2^2$ and $\underline{u} \equiv h_{e-2}(x)\underline{b}_0 \equiv h(x)\underline{a}_0 \bmod 2$.

Since $\underline{a}_0 = \underline{b}_0$, $\underline{v} + \underline{w} \equiv h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2$. By (7) and (8),

$$(x^{2^{e-3}T} - 1)(\underline{a}_{e-1} + \underline{b}_{e-1}) \equiv (\underline{a}_{e-2} + \underline{b}_{e-2})h(x)\underline{a}_0 + h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2. \tag{9}$$

Comparing with (5), it follows that

$$(\underline{a}_{e-2} + \underline{b}_{e-2})h(x)\underline{a}_0$$
$$\equiv h(x)(\underline{a}_1 + \underline{b}_1)[\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) + \eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})]h(x)\underline{a}_0 \bmod 2. \tag{10}$$

If $e \geq 5$, then $x^{2^{e-4}T} - 1 \equiv 2^{e-3} h_{e-3}(x) \bmod f(x)$ acts on $\underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1} 2^{e-1}$ and $\underline{b} = \underline{b}_0 + \underline{b}_1 2 + \cdots + \underline{b}_{e-1} 2^{e-1}$. It follows that

$$(x^{2^{e-4}T} - 1)(\underline{a}_{e-3} + \underline{a}_{e-2} 2) \equiv h_{e-3}(x)(\underline{a}_0 + \underline{a}_1 2) \bmod 2^2, \tag{11}$$

$$(x^{2^{e-4}T} - 1)(\underline{b}_{e-3} + \underline{b}_{e-2} 2) \equiv h_{e-3}(x)(\underline{b}_0 + \underline{b}_1 2) \bmod 2^2. \tag{12}$$

Similar to (9), we get

$$(x^{2^{e-4}T} - 1)(\underline{a}_{e-2} + \underline{b}_{e-2}) \equiv (\underline{a}_{e-3} + \underline{b}_{e-3}) h(x) \underline{a}_0 + h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2. \tag{13}$$

Multiplying (13) by $h(x)\underline{a}_0$, since $\mathrm{per}(h(x)\underline{a}_0)$ divides T, we obtain

$$\begin{aligned}&(x^{2^{e-4}T} - 1)[(\underline{a}_{e-2} + \underline{b}_{e-2}) h(x) \underline{a}_0] \\ &\equiv (\underline{a}_{e-3} + \underline{b}_{e-3}) h(x) \underline{a}_0 + h(x)(\underline{a}_1 + \underline{b}_1) h(x) \underline{a}_0 \bmod 2.\end{aligned} \tag{14}$$

By (10) and (3), we have

$$\begin{aligned}(\underline{a}_{e-2} + \underline{b}_{e-2}) h(x) \underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1)[&\underline{a}_{e-3} \eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) \\ &+ \underline{b}_{e-3} \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4}) + \psi_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) \\ &+ \psi_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})] h(x) \underline{a}_0 \bmod 2.\end{aligned}$$

It follows that

$$\begin{aligned}&(x^{2^{e-4}T} - 1)[(\underline{a}_{e-2} + \underline{b}_{e-2}) h(x) \underline{a}_0] \\ &\equiv (x^{2^{e-4}T} - 1)[\underline{a}_{e-3} \eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \underline{b}_{e-3} \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})] h(x) \underline{a}_0 \\ &\equiv [\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})] h(x) \underline{a}_0 \bmod 2.\end{aligned}$$

Comparing with (14), we get

$$\begin{aligned}(\underline{a}_{e-3} + \underline{b}_{e-3}) h(x) \underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1) h(x) \underline{a}_0 + [&\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) \\ &+ \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})] h(x) \underline{a}_0 \bmod 2.\end{aligned} \tag{15}$$

Now, we show $h(x)(\underline{a}_1 + \underline{b}_1) h(x) \underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2$. If $\underline{a}_1 = \underline{b}_1$, then

$$h(x)(\underline{a}_1 + \underline{b}_1) h(x) \underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1) \equiv \underline{0} \bmod 2.$$

If $\underline{a}_1 \neq \underline{b}_1$, then 0th level component of $\underline{a} - \underline{b}$ is $\underline{0}$ and 1th level component $\underline{a} - \underline{b}$ is $\underline{a}_1 + \underline{b}_1 \bmod 2$. Thus $\underline{a}_1 + \underline{b}_1$ is a primitive sequence generated by $f(x)$ over F_2, so is $h(x)(\underline{a}_1 + \underline{b}_1)$. Let $h(x)\underline{a}_0 = (u_0, u_1, u_2, \ldots)$ and

$h(x)(\underline{a}_1 + \underline{b}_1) = (s_0, s_1, s_2, \ldots)$ over F_2, then by (10), $s_i = 0$ if $u_i = 0$. And since $h(x)(\underline{a}_1 + \underline{b}_1)$ and $h(x)\underline{a}_0$ are primitive sequences generated by $f(x)$ over F_2, we get $h(x)\underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2$, that is $\underline{a}_1 + \underline{b}_1 \equiv \underline{a}_0 \bmod 2$. So

$$h(x)(\underline{a}_1 + \underline{b}_1)h(x)\underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2.$$

Then, (15) implies

$$(\underline{a}_{e-3} + \underline{b}_{e-3})h(x)\underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1) + [\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})]h(x)\underline{a}_0 \bmod 2.$$

In general, we have

$$(\underline{a}_{e-i} + \underline{b}_{e-i})h(x)\underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1) + [\eta_{e-i-1}(\underline{a}_0, \ldots, \underline{a}_{e-i-1}) + \eta_{e-i-1}(\underline{b}_0, \ldots, \underline{b}_{e-i-1})]h(x)\underline{a}_0 \bmod 2, \tag{16}$$

where $i = 2, 3, \ldots, e-2$. Finally, by $x^T - 1 \equiv 2h_1(x) \bmod f(x)$ acting on $\underline{a}$ and $\underline{b}$, similar to (9), we have

$$(x^T - 1)(\underline{a}_2 + \underline{b}_2) \equiv (\underline{a}_1 + \underline{b}_1)h_1(x)\underline{a}_0 + h_1(x)(\underline{a}_1 + \underline{b}_1) \bmod 2, \tag{17}$$

which implies

$$(x^T - 1)[(\underline{a}_2 + \underline{b}_2)h(x)\underline{a}_0] \equiv (\underline{a}_1 + \underline{b}_1)h_1(x)\underline{a}_0h(x)\underline{a}_0 + h_1(x)(\underline{a}_1 + \underline{b}_1)h(x)\underline{a}_0 \bmod 2. \tag{18}$$

On the other hand, by (16) in the case of $i = e-2$,

$$(\underline{a}_2 + \underline{b}_2)h(x)\underline{a}_0 \equiv h(x)(\underline{a}_1 + \underline{b}_1) + [\eta_1(\underline{a}_0, \underline{a}_1) + \eta_1(\underline{b}_0, \underline{b}_1)]h(x)\underline{a}_0 \bmod 2 \tag{19}$$

and $\eta_1(x_0, x_1) = x_1\eta_0(x_0) + \psi_0(x_0)$, we have

$$\begin{aligned}
&(x^T - 1)[(\underline{a}_2 + \underline{b}_2)h(x)\underline{a}_0] \\
&\equiv (x^T - 1)[(\eta_1(\underline{a}_0, \underline{a}_1) + \eta_1(\underline{b}_0, \underline{b}_1))h(x)\underline{a}_0 + h(x)(\underline{a}_1 + \underline{b}_1)] \\
&\equiv (x^T - 1)[\underline{a}_1\eta_0(\underline{a}_0) + \underline{b}_1\eta_0(\underline{b}_0)]h(x)\underline{a}_0 \\
&\equiv \eta_1(\underline{a}_0)h(x)\underline{a}_0(x^T - 1)(\underline{a}_1 + \underline{b}_1) \\
&\equiv \eta_1(\underline{a}_0)h(x)\underline{a}_0(h_1(x)\underline{a}_0 + h_1(x)\underline{b}_0) \equiv \underline{0} \bmod 2.
\end{aligned}$$

So (18) implies

$$(\underline{a}_1 + \underline{b}_1)h_1(x)\underline{a}_0h(x)\underline{a}_0 \equiv h_1(x)(\underline{a}_1 + \underline{b}_1)h(x)\underline{a}_0 \bmod 2.$$

If $\underline{a}_1 \neq \underline{b}_1$, then $\underline{a}_1 + \underline{b}_1 \equiv \underline{a}_0 \bmod 2$ and the above equation implies

$$\underline{a}_0 h_1(x)\underline{a}_0 h(x)\underline{a}_0 \equiv h_1(x)\underline{a}_0 h(x)\underline{a}_0 \bmod 2. \tag{20}$$

It is clear that $\underline{a}_0$, $h_1(x)\underline{a}_0$ and $h(x)\underline{a}_0$ are linear independent over F_2, since $h(x) \equiv h_1(x) + h_1(x)^2 \bmod 2$, $h_1(x) \not\equiv 0 \bmod 2$ and $h(x) \not\equiv 0, 1 \bmod 2$. So, by Lemma 4, (20) is not true. Thus $\underline{a}_1 = \underline{b}_1$ and by (19), $(\underline{a}_2 + \underline{b}_2)h(x)\underline{a}_0 \equiv \underline{0} \bmod 2$, which implies $\underline{a}_2 = \underline{b}_2$. And by (16) again, we have $(\underline{a}_{e-i} + \underline{b}_{e-i})h(x)\underline{a}_0 \equiv \underline{0} \bmod 2$, which implies $\underline{a}_{e-i} = \underline{b}_{e-i}$, $i = e-3$, $e-4, \ldots, 2$. Finally $\underline{a}_{e-1} = \underline{b}_{e-1}$ since $\underline{a}_k = \underline{b}_k$, $k = 0, 1, \ldots, e-2$, and $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$. Therefore, $\underline{a} = \underline{b}$.

Secondly, we consider the case $e = 3$. We have $\varphi(x_0, x_1, x_2) = x_2 + \eta(x_0, x_1)$ and $\eta(x_0, x_1) = x_1\eta_0(x_0) + \psi_0(x_0)$. Since $\varphi(\underline{a}_0, \underline{a}_1, \underline{a}_2) \equiv \varphi(\underline{b}_0, \underline{b}_1, \underline{b}_2)$ and $\underline{a}_0 = \underline{b}_0$, it follows that

$$\underline{a}_2 + \underline{b}_2 \equiv (\underline{a}_1 + \underline{b}_1)\eta_0(\underline{a}_0) \bmod 2. \tag{21}$$

By Lemmas 3 and 2,

$$\begin{aligned}(x^T - 1)(\underline{a}_2 + \underline{b}_2) &\equiv (x^T - 1)((\underline{a}_1 + \underline{b}_1)\eta_0(\underline{a}_0)) \\ &\equiv \eta_0(\underline{a}_0)(x^T - 1)(\underline{a}_1 + \underline{b}_1) \\ &\equiv \eta_0(\underline{a}_0)(h_1(x)\underline{a}_0 + h_1(x)\underline{b}_0) \equiv \underline{0} \bmod 2.\end{aligned}$$

By (17), we have

$$h_1(x)(\underline{a}_1 + \underline{b}_1) \equiv (\underline{a}_1 + \underline{b}_1)h_1(x)\underline{a}_0 \bmod 2.$$

If $\underline{a}_1 + \underline{b}_1 \not\equiv \underline{0} \bmod 2$, then $\underline{a}_1 + \underline{b}_1 \bmod 2$ is a primitive sequence over F_2; and since $h_1(x) \not\equiv \underline{0} \bmod 2$, $h_1(x)(\underline{a}_1 + \underline{b}_1)$ and $h_1(x)\underline{a}_0$ are also primitive sequences over F_2. This condition is in contradiction with the above equation. So $\underline{a}_1 + \underline{b}_1 \equiv \underline{0} \bmod 2$, and by (21), we have $\underline{a}_2 = \underline{b}_2$ and $\underline{a} = \underline{b}$.

Finally, considering the case $e = 2$, we have $\varphi(x_0, x_1) = x_1 + \eta(x_0)$. So $\varphi(\underline{a}_0, \underline{a}_1) \equiv \varphi(\underline{b}_0, \underline{b}_1) \bmod 2$ and $\underline{a}_0 = \underline{b}_0$ imply $\underline{a}_1 = \underline{b}_1$. Hence $\underline{a} = \underline{b}$. ■

3. COMPRESSION MAPPINGS OVER GALOIS RINGS

Let p be a prime, Z_p the p-adic integer ring and Q_p the p-adic number field. Let K be an unramified extension of Q_p with degree r, R the integer ring of K, then $GR(p^e, r) = R/p^eR$ is called a Galois ring, where e is a positive integer.

Remark 2. (1) Let $g(x)$ be a monic polynomial over $Z/(p^e)$ with degree r. If $g(x) \bmod p$ is irreducible over F_p, then $A[x]/(g(x)) \cong GR(p^e, r)$, where $A = Z/(p^e)$.

(2) $GR(p^e, 1) = Z/(p^e)$.

(3) $GR(p^e, r)$ is a local ring with the maximal ideal

$$(p) = pGR(p^e, r) = \{p\alpha \mid \alpha \in GR(p^e, r)\}$$

and $GR(p, r) = GR(p^e, r)/(p) = F_{p^r}$ is a finite field of p^r elements.

(4) Let $\Omega = \{\alpha \in GR(p^e, r) | \alpha^{p^r} = \alpha\}$, then Ω consists of p^r elements, which are distinct modulo p. So the mapping $\Omega \to F_{p^r}$, $\alpha \mapsto \alpha \bmod p$ is bijective. Furthermore, each element α in $GR(p^e, r)$ may be written uniquely as

$$\alpha = \alpha_0 + \alpha_1 p + \cdots + \alpha_{e-1} p^{e-1},$$

where $\alpha_i \in \Omega$. We call Ω the p-adic coordinate set of $GR(p^e, r)$ (see [5]).

(5) Let $\underline{a}$ be a sequence over $GR(p^e, r)$, then $\underline{a}$ may be written uniquely as

$$\underline{a} = \underline{a}_0 + \underline{a}_1 p + \cdots + \underline{a}_{e-1} p^{e-1},$$

where $\underline{a}_i = (a_{i0}, a_{i1}, \ldots)$ is a sequence over Ω, $i = 0, 1, \ldots, e-1$. The sequence $\underline{a}_i$ is called ith level component of $\underline{a}$ and $\underline{a}_{e-1}$ the highest level component of $\underline{a}$.

Now we set $p = 2$ and let $f(x)$ be a monic polynomial over $GR(2^e, r)$. If $f(0) \not\equiv 0 \bmod 2$, then there exists a positive integer P such that $f(x)$ divides $x^P - 1$ and the least such P is called the period of $f(x)$ over $GR(2^e, r)$, denoted by $\mathrm{per}(f(x))$. For a monic polynomial $f(x)$ over $GR(2^e, r)$ with degree n, the period of $f(x)$ is upper bounded by $2^{e-1}(2^{rn} - 1)$ and $f(x)$ is called a primitive polynomial if $\mathrm{per}(f(x)) = 2^{e-1}(2^{rn} - 1)$. Let $f(x)$ be a primitive polynomial of degree n over $GR(2^e, r)$, then $f(x) \bmod 2$ is a primitive polynomial over F_{2^r}. Let $\underline{a}$ be a sequence over $GR(2^e, r)$, generated by a primitive polynomial $f(x)$ of degree n with $\underline{a} \not\equiv \underline{0} \bmod 2$, then $\mathrm{per}(\underline{a}) = \mathrm{per}(f(x)) = 2^{e-1}T$ and $\mathrm{per}(\underline{a}_i) = 2^i T$ where $T = 2^{rn} - 1$, $i = 0, 1, \ldots, e-1$. Especially $\mathrm{per}(\underline{a}_{e-1}) = \mathrm{per}(\underline{a}) = 2^{e-1}T$.

LEMMA 6. *Let $f(x)$ be a primitive polynomial of degree n over $GR(2^e, r)$, $T = 2^{rn} - 1$, then there exists $h_i(x)$ over $GR(2^e, r)$ of degree less than n, $i = 1, 2, \ldots, e-1$, such that*

$$x^{2^{i-1}T} - 1 \equiv 2^i h_i(x) \bmod f(x). \tag{22}$$

Furthermore, all $h_i(x) \not\equiv 0 \bmod 2$, $h_2(x) \equiv \cdots \equiv h_{e-1}(x) \bmod 2$ and $h_2(x) \equiv h_1(x) + h_1(x)^2 \bmod (2, f(x))$.

DEFINITION 1. Let $f(x)$ be a primitive polynomial over $\mathrm{GR}(2^e, r)$. If $e \geq 3$ and $\deg(h_2(x) \bmod 2) \geq 1$ or $e = 2$ and $\deg(h_1(x) \bmod 2) \geq 1$, then $f(x)$ is called a strongly primitive polynomial over $\mathrm{GR}(2^e, r)$.

LEMMA 7. *Let $f(x)$ be a primitive polynomial over $\mathrm{GR}(2^e, r)$, $\eta(x_0, x_1, \ldots, x_{e-2})$ a function of $e-1$ variables over F_{2^r} and*

$$\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2}).$$

For $\underline{a}, \underline{b} \in G(f(x), \mathrm{GR}(2^e, r))$, if $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$, then $\underline{a}_0 = \underline{b}_0$.

The proof is similar to the one of Lemma 5.

LEMMA 8. *Let Ω be the p-adic coordinate set of $\mathrm{GR}(2^e, r)$, $\delta \in \mathrm{GR}(2^e, r)$, $\alpha, \beta \in \Omega$, then*

1. $\delta^{2^r} \equiv \delta \bmod 2$.
2. *For $s \geq e-1$, $\delta^{2^s} \in \Omega$.*
3. $\alpha\beta \in \Omega$.
4. *Let s be a positive integer such that $rs \geq e-1$, then $(\alpha+\beta)^{2^{rs}} \in \Omega$, $(\alpha\beta)^{2^{r-1}} \in \Omega$ and*

$$\alpha + \beta \equiv (\alpha+\beta)^{2^{rs}} + 2(\alpha\beta)^{2^{r-1}} \qquad \bmod 2^2.$$

Proof. (1) Let $\delta = \lambda + 2\xi$, where $\lambda \in \Omega$, $\xi \in \mathrm{GR}(2^e, r)$. Since $\lambda^{2^r} = \lambda$, $\delta^{2^r} \equiv \delta \bmod 2$.

(2) If $\delta \equiv 0 \bmod 2$, then $\delta = 2\xi$, where $\xi \in \mathrm{GR}(2^e, r)$. Since $2^s \geq 2^{e-1} \geq e$, we have $\delta^{2^s} = 0 \in \Omega$. If $\delta \not\equiv 0 \bmod 2$, then $\delta = \lambda + 2\xi$, where $\lambda \in \Omega$, $\xi \in \mathrm{GR}(2^e, r)$. So $\delta^{2^s} = (\lambda + 2\xi)^{2^s} = \lambda^{2^s} + 2^{1+s}\lambda^{2^s-1}\xi + \cdots = \lambda^{2^s} \in \Omega$.

(3) $(\alpha\beta)^{2^r} = \alpha^{2^r}\beta^{2^r} = \alpha\beta$, so $\alpha\beta \in \Omega$.

(4) By (2) and (3), $(\alpha+\beta)^{2^{rs}} \in \Omega$, $(\alpha\beta)^{2^{r-1}} \in \Omega$. Since

$$(\alpha+\beta)^{2^k} \equiv \alpha^{2^k} + \beta^{2^k} + 2\alpha^{2^{k-1}}\beta^{2^{k-1}} \bmod 2^2,$$

we have

$$\begin{aligned}(\alpha+\beta)^{2^{rs}} &\equiv \alpha^{2^{rs}} + \beta^{2^{rs}} + 2\alpha^{2^{rs-1}}\beta^{2^{rs-1}} \\ &\equiv \alpha + \beta + 2(\alpha^{2^{r(s-1)}})^{2^{r-1}}(\beta^{2^{r(s-1)}})^{2^{r-1}} \\ &\equiv \alpha + \beta + 2(\alpha\beta)^{2^{r-1}} \bmod 2^2.\end{aligned}$$

So $\alpha + \beta \equiv (\alpha+\beta)^{2^{rs}} + 2(\alpha\beta)^{2^{r-1}} \bmod 2^2$. ∎

LEMMA 9. *Let $f(x)$ be a primitive polynomial of degree n over the finite field F_{2^r}, $\underline{u} = (u_0, u_1, \ldots)$, $\underline{v} = (v_0, v_1, \ldots) \in G(f(x), F_{2^r})$ and $\underline{v} \neq \underline{0}$. If $v_i = 0$ implies $u_i = 0$, then there exists $c \in F_{2^r}$ such that $\underline{u} = c\,\underline{v}$.*

Proof. If $\underline{u} = \underline{0}$, then we set $c = 0$ and get $\underline{u} = c\underline{v}$. Now assume $\underline{u} \neq \underline{0}$, then $\underline{v} \neq \underline{0}$ by the condition. Since $f(x)$ is a primitive polynomial of degree n and $\underline{u}$ and $\underline{v}$ are generated by $f(x)$, there exists a nonnegative integer k such that $(u_k, u_{k+1}, \ldots, u_{k+n-1}) = (0, 0, \ldots, 0, a)$ and $(v_k, v_{k+1}, \ldots, v_{k+n-1}) = (0, 0, \ldots, 0, b)$, where $a \neq 0$ and $b \neq 0$. Then it is clear that $\underline{u} = c\underline{v}$, where $c = ab^{-1}$. ■

LEMMA 10. *Let $f(x)$ be a primitive polynomial of degree n over $GR(2^e, r)$, $T = 2^{rn} - 1$, $\underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1} 2^{e-1} \in G(f(x), GR(2^e, r))$ and $\underline{a}_0 \neq \underline{0}$, then $\mathrm{per}(\underline{a}_i) = 2^i T$, especially $\mathrm{per}(\underline{a}_{e-1}) = 2^{e-1} T = \mathrm{per}(\underline{a}) = \mathrm{per}(f(x))$.*

The proof is similar to one of Lemma 1 cited from [1].

LEMMA 11. *Let $f(x)$ be a strongly primitive polynomial over $GR(2^e, r)$, $e \geq 3$, $\underline{a}, \underline{b} \in G(f(x), GR(2^e, r))$ and $\underline{a}_0 = \underline{b}_0 \neq \underline{0}$. If there exists $c \in F_{2^r}$ such that $\underline{a}_1 + \underline{b}_1 \equiv c\underline{a}_0 \bmod 2$ and*

$$\underline{a}_0 h_1(x)\underline{a}_0 (h_2(x)\underline{a}_0)^2 \equiv c(h_1(x)(\underline{a}_0))^2 (h_2(x)\underline{a}_0)^2 \bmod 2, \tag{23}$$

where $h_1(x)$ and $h_2(x)$ is defined by (22), then $\underline{a}_1 = \underline{b}_1$, i.e. $c = 0$.

Proof. Assume $\underline{a}_1 \neq \underline{b}_1$, that is, $c \neq 0$.

If $\underline{a}_0$, $h_1(x)\underline{a}_0$ and $h_2(x)\underline{a}_0$ are linear independent over F_{2^r}, then, by Lemma 4,

$$\underline{a}_0 h_1(x)\underline{a}_0 (h_2(x)\underline{a}_0)^2 \not\equiv c(h_1(x)(\underline{a}_0))^2 (h_2(x)\underline{a}_0)^2 \bmod 2,$$

that is a contradiction. Now suppose that $\underline{a}_0$, $h_1(x)\underline{a}_0$ and $h_2(x)\underline{a}_0$ are linear dependent over F_{2^r}. Since $\underline{a}_0$ is an m-sequence generated by $f(x)$ over F_{2^r}, $\deg(h_1(x) \bmod 2) \geq 1$, $\deg(h_2(x) \bmod 2) \geq 1$ and $h_1(x) \not\equiv h_2(x) \bmod 2$, we conclude that any two of $\underline{a}_0$, $h_1(x)\underline{a}_0$ and $h_2(x)\underline{a}_0$ are linear independent over F_{2^r}. Thus, we can assume $\underline{a}_0 = c_1 h_1(x)\underline{a}_0 + c_2 h_2(x)\underline{a}_0$ over F_{2^r}, where c_1 and c_2 are nonzero elements in F_{2^r}. We write $\underline{a}_0 = (\alpha_0, \alpha_1, \alpha_2, \ldots)$, $c_1 h_1(x)\underline{a}_0 = (\beta_0, \beta_1, \beta_2, \ldots)$, $c_2 h_2(x)\underline{a}_0 = (\gamma_0, \gamma_1, \gamma_2, \ldots)$ over F_{2^r}. Since $c_1 h_1(x)\underline{a}_0$ and $c_2 h_2(x)\underline{a}_0$ are linear independent over F_{2^r}, there exists nonnegative integer t such that $\beta_t = \gamma_t \neq 0$. Then $\theta_t \neq 0$ in $c(h_1(x)(\underline{a}_0))^2 (h_2(x)\underline{a}_0)^2 = (\theta_0, \theta_1, \theta_2, \ldots)$. But $\alpha_t = \beta_t + \gamma_t = 2\beta_t = 0$, by (23), we get a contradiction. ■

LEMMA 12. *Let $g(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 \in F_{2^r}[x]$, $f(x) = c_n^2 x^n + c_{n-1}^2 x^{n-1} + \cdots + c_0^2$ and $\underline{u}$ a sequence over F_{2^r}. Then $(g(x)\underline{u})^2 = f(x)\underline{u}^2$. Especially, $((x^k - 1)\underline{u})^2 = (x^k - 1)(\underline{u}^2)$ for any positive integer k.*

The proof is easy.

THEOREM 3. *Let $f(x)$ be a strongly primitive polynomial of degree n over* $\mathrm{GR}(2^e, r)$, $\varphi(x_0, x_1, \ldots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \ldots, x_{e-2})$, *where* $\eta(x_0, x_1, \ldots, x_{e-2})$ *is a function of* $e-1$ *variables over* F_{2^r}. *Set* $\eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) = \eta(x_0, x_1, \ldots, x_{e-2})$. *If* $\eta_{e-2}(x_0, x_1, \ldots, x_{e-2})$ *satisfies*

$$\eta_{e-2}(x_0, x_1, \ldots, x_{e-2}) = x_{e-2}\eta_{e-3}(x_0, x_1, \ldots, x_{e-3}) + \psi_{e-3}(x_0, x_1, \ldots, x_{e-3})$$

and

$$\eta_i(x_0, x_1, \ldots, x_i) = x_i\eta_{i-1}(x_0, x_1, \ldots, x_{i-1}) + \psi_{i-1}(x_0, x_1, \ldots, x_{i-1}),$$

where $i = 1, 2, \ldots, e-2$, $\eta_{i-1}(x_0, x_1, \ldots, x_{i-1})$ *and* $\psi_{i-1}(x_0, x_1, \ldots, x_{i-1})$ *are functions of i variables over* F_{2^r}, *then the compression mapping*

$$\Phi: \begin{cases} G(f(x), \mathrm{GR}(2^e, r)) \to F_{2^r}^{\infty}, \\ \underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1}2^{e-1} \mapsto \varphi(\underline{a}_0, \underline{a}_1, \ldots, \underline{a}_{e-1}) \bmod 2 \end{cases}$$

is injective, that is, for $\underline{a}, \underline{b} \in G(f(x), \mathrm{GR}(2^e, r))$, $\underline{a} = \underline{b}$ *if and only if* $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2$.

Proof. Let $\underline{a}, \underline{b} \in G(f(x), \mathrm{GR}(2^e, r))$ satisfying

$$\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) \equiv \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1}) \bmod 2.$$

By Lemma 7, $\underline{a}_0 = \underline{b}_0$. It is not harmful to assume $\underline{a}_0 \neq \underline{0}$.

(1) Assume $e \geq 4$. Since $h_2(x) \equiv \cdots \equiv h_{e-1}(x) \bmod 2$, we set $h(x) = h_i(x) \bmod 2$ over F_{2^r}, $2 \leq i \leq e-1$.

Since

$$\begin{aligned} &\underline{a}_{e-1} + \underline{a}_{e-2}\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) + \psi_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) \\ &\equiv \underline{b}_{e-1} + \underline{b}_{e-2}\eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3}) + \psi_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3}) \bmod 2 \end{aligned} \tag{24}$$

and by Lemma 10 the periods of $\psi_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3})$ and $\psi_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})$ divide $2^{e-3}T$, where $T = 2^{rn} - 1$, by $x^{2^{e-3}T} - 1$ acting on (24), we can get

$$\begin{aligned} &(x^{2^{e-3}T} - 1)(\underline{a}_{e-1} + \underline{a}_{e-2}\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3})) \\ &\equiv (x^{2^{e-3}T} - 1)(\underline{b}_{e-1} + \underline{b}_{e-2}\eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})) \bmod 2. \end{aligned} \tag{25}$$

Furthermore, by Lemma 3, we have

$$\begin{aligned} &(x^{2^{e-3}T} - 1)\underline{a}_{e-1} + \eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3})(x^{2^{e-3}T} - 1)\underline{a}_{e-2} \\ &\equiv (x^{2^{e-3}T} - 1)\underline{b}_{e-1} + \eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})(x^{2^{e-3}T} - 1)\underline{b}_{e-2} \bmod 2. \end{aligned} \tag{26}$$

Since $\underline{a}_0 = \underline{b}_0$ and by Lemma 6 $x^{2^{e-3}T} - 1 \equiv 2^{e-2}h_{e-2}(x) \bmod f(x)$, it follows that

$$(x^{2^{e-3}T} - 1)\underline{a}_{e-2} \equiv h(x)\underline{a}_0 \equiv h(x)\underline{b}_0 \equiv (x^{2^{e-3}T} - 1)\underline{b}_{e-2} \bmod 2.$$

So (26) implies that

$$\begin{aligned}&(x^{2^{e-3}T} - 1)(\underline{a}_{e-1} + \underline{b}_{e-1})\\ &\equiv [\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) + \eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})]h(x)\underline{a}_0 \bmod 2. \end{aligned} \tag{27}$$

By $x^{2^{e-3}T} - 1 \equiv 2^{e-2}h_{e-2}(x) \bmod f(x)$ acting on $\underline{a} = \underline{a}_0 + \underline{a}_1 2 + \cdots + \underline{a}_{e-1}2^{e-1}$,

$$(x^{2^{e-3}T} - 1)(\underline{a}_{e-2} + \underline{a}_{e-1}2) \equiv h_{e-2}(x)(\underline{a}_0 + \underline{a}_1 2) \bmod 2^2. \tag{28}$$

Let

$$h_{e-2}(x)(\underline{a}_0 + \underline{a}_1 2) \equiv \underline{u} + \underline{v}2 \bmod 2^2, \tag{29}$$

where $\underline{u}$ and $\underline{v}$ are 0th and 1th level components of $h_{e-2}(x)(\underline{a}_0 + \underline{a}_1 2)$, respectively. It is clear that $\underline{u} \equiv h_{e-2}(x)\underline{a}_0 \bmod 2$. So, by (28)

$$x^{2^{e-3}T}\underline{a}_{e-2} + (x^{2^{e-3}T} - 1)\underline{a}_{e-1}2 \equiv \underline{a}_{e-2} + \underline{u} + v2 \bmod 2^2. \tag{30}$$

By Lemma 8, $\underline{a}_{e-2} + \underline{u} \equiv (\underline{a}_{e-2} + \underline{u})^{2^{rs}} + 2(\underline{a}_{e-2}\underline{u})^{2^{r-1}} \bmod 2^2$, where s is a positive integer such that $rs \geq e - 1$. Since $(\underline{a}_{e-2} + \underline{u})^{2^{rs}}$ is a sequence over Ω, by (30), it follows that

$$(x^{2^{e-3}T} - 1)\underline{a}_{e-1} \equiv \underline{v} + (\underline{u}\underline{a}_{e-2})^{2^{r-1}} \bmod 2. \tag{31}$$

Similarly, we have

$$(x^{2^{e-3}T} - 1)\underline{b}_{e-1} \equiv \underline{w} + (\underline{u}\underline{b}_{e-2})^{2^{r-1}} \bmod 2, \tag{32}$$

where $\underline{w}$ is determined by

$$h_{e-2}(x)(\underline{b}_0 + \underline{b}_1 2) \equiv \underline{u} + \underline{w}2 \bmod 2^2. \tag{33}$$

Since $\underline{a}_0 = \underline{b}_0$, by (29) and (33), it follows that $\underline{v} + \underline{w} = h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2$, and by (31) and (32), we have

$$(x^{2^{e-3}T} - 1)(\underline{a}_{e-1} + \underline{b}_{e-1}) \equiv \underline{u}^{2^{r-1}}(\underline{a}_{e-2} + \underline{b}_{e-2})^{2^{r-1}} + h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2. \tag{34}$$

By (27) and $\underline{u} \equiv h(x)\underline{a}_0 \bmod 2$,

$$\underline{u}^{2^{r-1}}(\underline{a}_{e-2} + \underline{b}_{e-2})^{2^{r-1}} \equiv [\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) + \eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})]\underline{u} + h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2. \quad (35)$$

Then

$$\begin{aligned}\underline{u}(\underline{a}_{e-2} + \underline{b}_{e-2}) &\equiv [\underline{u}^{2^{r-1}}(\underline{a}_{e-2} + \underline{b}_{e-2})^{2^{r-1}}]^2 \\ &\equiv [\eta_{e-3}(\underline{a}_0, \ldots, \underline{a}_{e-3}) + \eta_{e-3}(\underline{b}_0, \ldots, \underline{b}_{e-3})]^2\underline{u}^2 \\ &\quad + [h(x)(\underline{a}_1 + \underline{b}_1)]^2 \bmod 2. \end{aligned} \quad (36)$$

If $e \geq 5$, $x^{2^{e-4}T} - 1 \equiv 2^{e-3}h_{e-3}(x) \bmod f(x)$ acts on $\underline{a}$ and $\underline{b}$ continuously. Then

$$(x^{2^{e-4}T} - 1)(\underline{a}_{e-3} + \underline{a}_{e-2}2) \equiv h_{e-3}(x)(\underline{a}_0 + \underline{a}_1 2) \bmod 2^2,$$

$$(x^{2^{e-4}T} - 1)(\underline{b}_{e-3} + \underline{b}_{e-2}2) \equiv h_{e-3}(x)(\underline{b}_0 + \underline{b}_1 2) \bmod 2^2.$$

Similar to (34), we have

$$(x^{2^{e-4}T} - 1)(\underline{a}_{e-2} + \underline{b}_{e-2}) \equiv \underline{u}^{2^{r-1}}(\underline{a}_{e-3} + \underline{b}_{e-3})^{2^{r-1}} + h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2 \quad (37)$$

and so

$$[(x^{2^{e-4}T} - 1)(\underline{a}_{e-2} + \underline{b}_{e-2})]\underline{u} \equiv \underline{u}[\underline{u}^{2^{r-1}}(\underline{a}_{e-3} + \underline{b}_{e-3})^{2^{r-1}} + h(x)(\underline{a}_1 + \underline{b}_1)] \bmod 2.$$

Since $\mathrm{per}(\underline{u}) = T$, we have

$$\begin{aligned}&(x^{2^{e-4}T} - 1)[(\underline{a}_{e-2} + \underline{b}_{e-2})\underline{u}] \\ &\equiv \underline{u}\underline{u}^{2^{r-1}}(\underline{a}_{e-3} + \underline{b}_{e-3})^{2^{r-1}} + \underline{u}h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2. \end{aligned} \quad (38)$$

And by (36), it follows that

$$(\underline{a}_{e-2} + \underline{b}_{e-2})\underline{u}$$

$$\equiv \underline{u}^2[\underline{a}_{e-3}\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \underline{b}_{e-3}\eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})$$

$$+ \psi_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \psi_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})]^2 + [h(x)(\underline{a}_1 + \underline{b}_1)]^2 \bmod 2.$$

The periods of $(\psi_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \psi_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4}))^2\underline{u}^2$ and $(h(x)(\underline{a}_1 + \underline{b}_1))^2$ divide $2^{e-4}T$, so it follows that

$$(x^{2^{e-4}T} - 1)[(\underline{a}_{e-2} + \underline{b}_{e-2})\underline{u}]$$

$$\equiv (x^{2^{e-4}T} - 1)[\underline{a}_{e-3} \cdot \eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \underline{b}_{e-3} \cdot \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})]^2\underline{u}^2 \bmod 2.$$

Comparing with (38) and by Lemma 12 we get

$$[\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4})(x^{2^{e-4}T} - 1)\underline{a}_{e-3} + \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})(x^{2^{e-4}T} - 1)\underline{b}_{e-3}]^2\underline{u}^2$$

$$\equiv \underline{u} \cdot \underline{u}^{2^{r-1}}(\underline{a}_{e-3} + \underline{b}_{e-3})^{2^{r-1}} + \underline{u} \cdot h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2.$$

Since $(x^{2^{e-4}T} - 1)\underline{a}_{e-3} \equiv h_{e-3}(x)\underline{a}_0 \equiv \underline{u} \bmod 2$, then

$$[\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})]^2\underline{u}^4$$

$$\equiv \underline{u} \cdot \underline{u}^{2^{r-1}}(\underline{a}_{e-3} + \underline{b}_{e-3})^{2^{r-1}} + \underline{u} \cdot h(x)(\underline{a}_1 + \underline{b}_1) \bmod 2.$$

So

$$[\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})]^4\underline{u}^8$$

$$\equiv [\underline{u} \cdot \underline{u}^{2^{r-1}}(\underline{a}_{e-3} + \underline{b}_{e-3})^{2^{r-1}} + \underline{u} \cdot h(x)(\underline{a}_1 + \underline{b}_1)]^2$$

$$\equiv \underline{u}^2 \cdot \underline{u}(\underline{a}_{e-3} + \underline{b}_{e-3}) + \underline{u}^2[h(x)(\underline{a}_1 + \underline{b}_1)]^2 \bmod 2,$$

that is,

$$\underline{u}(\underline{a}_{e-3} + \underline{b}_{e-3})\underline{u}^2 \equiv [\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})]^4\underline{u}^8 + \underline{u}^2[h(x)(\underline{a}_1 + \underline{b}_1)]^2 \bmod 2. \tag{39}$$

Let $\underline{u} \equiv (u_0, u_1, \ldots) \bmod 2$, $h(x)(\underline{a}_1 + \underline{b}_1) = (w_0, w_1, \ldots) \bmod 2$, by (36), it follows that if $u_i = 0$, then $w_i \equiv 0$. So by Lemma 9, $h(x)(\underline{a}_1 + \underline{b}_1) \equiv c\underline{u} \bmod 2$

for some $c \in \mathrm{F}_{2^r}$, and (39) implies

$$\underline{u}(\underline{a}_{e-3} + \underline{b}_{e-3}) \equiv \underline{u}^6[\eta_{e-4}(\underline{a}_0, \ldots, \underline{a}_{e-4}) + \eta_{e-4}(\underline{b}_0, \ldots, \underline{b}_{e-4})]^4 + [h(x)(\underline{a}_1 + \underline{b}_1)]^2 \bmod 2.$$

From the above discussion, we deduce the following formula:

$$\underline{u}(\underline{a}_{e-i} + \underline{b}_{e-i}) \equiv \underline{u}^{k_i}(\eta_{e-i-1}(\underline{a}_0, \ldots, \underline{a}_{e-i-1}) + \eta_{e-i-1}(\underline{b}_0, \ldots, \underline{b}_{e-i-1}))^{2^{i-1}} + [h(x)(\underline{a}_1 + \underline{b}_1)]^2 \bmod 2, \tag{40}$$

where k_i is a positive integer, $i = 2, 3, \ldots, e-2$. Take $i = e-2$, then

$$\underline{u}(\underline{a}_2 + \underline{b}_2) \equiv \underline{u}^{k_{e-2}}[\eta_1(\underline{a}_0, \underline{a}_1) + \eta_1(\underline{b}_0, \underline{b}_1)]^{2^{e-3}} + [h(x)(\underline{a}_1 + \underline{b}_1)]^2 \bmod 2. \tag{41}$$

Finally, $x^T - 1 \equiv 2h_1(x) \bmod f(x)$ acts on $\underline{a}$ and $\underline{b}$. Similar to (34), we have

$$(x^T - 1)(\underline{a}_2 + \underline{b}_2) \equiv (h_1(x)\underline{a}_0)^{2^{r-1}}(\underline{a}_1 + \underline{b}_1)^{2^{r-1}} + h_1(x)(\underline{a}_1 + \underline{b}_1) \bmod 2, \tag{42}$$

which deduces

$$(x^T - 1)(\underline{a}_2 + \underline{b}_2)\underline{u} \equiv (h_1(x)\underline{a}_0)^{2^{r-1}}(\underline{a}_1 + \underline{b}_1)^{2^{r-1}}\underline{u} + h_1(x)(\underline{a}_1 + \underline{b}_1)\underline{u} \bmod 2. \tag{43}$$

Since $\eta_1(x_0, x_1) = x_1\eta_0(x_0) + \psi_0(x_0)$ and $h(x)(\underline{a}_1 + \underline{b}_1) \equiv c\underline{u} \bmod 2$, (41) implies

$$(x^T - 1)(\underline{a}_1 \cdot \eta_0(\underline{a}_0) + \underline{b}_1 \cdot \eta_0(\underline{b}_0))^{2^{e-3}}\underline{u}^{k_{e-2}} \equiv (h_1(x)\underline{a}_0)^{2^{r-1}}(\underline{a}_1 + \underline{b}_1)^{2^{r-1}}\underline{u} + h_1(x)(\underline{a}_1 + \underline{b}_1)\underline{u} \bmod 2. \tag{44}$$

Since $(x^T - 1)\underline{a}_1 \equiv (x^T - 1)\underline{b}_1 \equiv h_1(x)\underline{a}_0 \bmod 2$ and $\eta_0(\underline{a}_0) \equiv \eta_0(\underline{b}_0) \bmod 2$, we have

$$(x^T - 1)(\underline{a}_1 \cdot \eta_0(\underline{a}_0) + \underline{b}_1 \cdot \eta_0(\underline{b}_0))^{2^{e-3}}\underline{u}^{k_{e-2}} \equiv [(x^T - 1)\underline{a}_1 \cdot \eta_0(\underline{a}_0) + (x^T - 1)\underline{b}_1 \cdot \eta_0(\underline{b}_0)]^{2^{e-3}}\underline{u}^{k_{e-2}} \equiv \underline{0} \bmod 2.$$

So (44) implies

$$(h_1(x)\underline{a}_0)^{2^{r-1}}(\underline{a}_1+\underline{b}_1)^{2^{r-1}}\underline{u}+h_1(x)(\underline{a}_1+\underline{b}_1)\underline{u}\equiv 0 \bmod 2$$

and then

$$\begin{aligned}(h_1(x)(\underline{a}_1+\underline{b}_1))^2\underline{u}^2 &\equiv [(h_1(x)\underline{a}_0)^{2^{r-1}}(\underline{a}_1+\underline{b}_1)^{2^{r-1}}\underline{u}]^2\\ &\equiv h_1(x)\underline{a}_0(\underline{a}_1+\underline{b}_1)\underline{u}^2 \bmod 2. \end{aligned} \tag{45}$$

Because $h(x)(\underline{a}_1+\underline{b}_1)\equiv c\underline{u} \bmod 2$ and $h_2(x)\underline{a}_0\equiv \underline{u} \bmod 2$, $h(x)(\underline{a}_1+\underline{b}_1)\equiv ch(x)\underline{a}_0\equiv h(x)(c\underline{a}_0)$, which implies $\underline{a}_1+\underline{b}_1\equiv c\underline{a}_0 \bmod 2$. And (45) implies that

$$\underline{a}_0\cdot h_1(x)\underline{a}_0(h_2(x)\underline{a}_0)^2\equiv c(h_1(x)(\underline{a}_0))^2(h_2(x)\underline{a}_0)^2 \bmod 2.$$

By Lemma 11, we get $\underline{a}_1=\underline{b}_1$. Thus $\underline{u}(\underline{a}_2+\underline{b}_2)\equiv \underline{0} \bmod 2$ by (41). Since $\underline{a}_0=\underline{b}_0$, $\underline{a}_1=\underline{b}_1$, it follows that $\underline{a}_2+\underline{b}_2$ is a primitive sequence over F_{2^r} or zero sequence. And since $\underline{u}$ is a primitive sequence over F_{2^r}, we get $\underline{a}_2+\underline{b}_2\equiv \underline{0} \bmod 2$, that is, $\underline{a}_2=\underline{b}_2$. So by (40), it follows that $\underline{a}_j=\underline{b}_j$, $j=3,\ldots,e-2$. Finally, by the condition $\varphi(\underline{a}_0,\ldots,\underline{a}_{e-1})\equiv\varphi(\underline{b}_0,\ldots,\underline{b}_{e-1}) \bmod 2$, we have $\underline{a}_{e-1}=\underline{b}_{e-1}$, and then $\underline{a}=\underline{b}$.

(2) Assume $e=3$, then $\varphi(x_0,x_1,x_2)=x_2+\eta(x_0,x_1)$ and $\eta(x_0,x_1)=x_1\eta_0(x_0)+\psi_0(x_0)$. Since $\varphi(\underline{a}_0,\underline{a}_1,\underline{a}_2)\equiv\varphi(\underline{b}_0,\underline{b}_1,\underline{b}_2)$ and $\underline{a}_0=\underline{b}_0$, it follows that

$$\underline{a}_2+\underline{b}_2\equiv(\underline{a}_1+\underline{b}_1)\eta_0(\underline{a}_0) \bmod 2. \tag{46}$$

By Lemmas 3 and 6,

$$\begin{aligned}(x^T-1)(\underline{a}_2+\underline{b}_2) &\equiv (x^T-1)((\underline{a}_1+\underline{b}_1)\eta_0(\underline{a}_0))\\ &\equiv \eta_0(\underline{a}_0)(x^T-1)(\underline{a}_1+\underline{b}_1)\\ &\equiv \eta_0(\underline{a}_0)(h_1(x)\underline{a}_0+h_1(x)\underline{b}_0)\\ &\equiv \underline{0} \bmod 2.\end{aligned}$$

By (42), we have $h_1(x)(\underline{a}_1+\underline{b}_1)\equiv(\underline{a}_1+\underline{b}_1)^{2^{r-1}}(h_1(x)\underline{a}_0)^{2^{r-1}} \bmod 2$, and so

$$\begin{aligned}(h_1(x)(\underline{a}_1+\underline{b}_1))^2 &\equiv [(\underline{a}_1+\underline{b}_1)^{2^{r-1}}(h_1(x)\underline{a}_0)^{2^{r-1}}]^2\\ &\equiv (\underline{a}_1+\underline{b}_1)h_1(x)\underline{a}_0 \bmod 2.\end{aligned}$$

If $\underline{a}_1+\underline{b}_1\not\equiv\underline{0} \bmod 2$, that is, $\underline{a}_1+\underline{b}_1 \bmod 2$ and $h_1(x)(\underline{a}_1+\underline{b}_1)$ are primitive sequences over F_{2^r}. Since $\deg(h_1(x) \bmod 2)\geq 1$, it

follows that and $\underline{a}_1 + \underline{b}_1 \equiv \underline{0} \bmod 2$; Furthermore, by (46), $\underline{a}_2 = \underline{b}_2$ and $\underline{a} = \underline{b}$.

(3) Assume $e = 2$, then $\varphi(x_0, x_1) = x_1 + \eta(x_0)$. So $\varphi(\underline{a}_0, \underline{a}_1) \equiv \varphi(\underline{b}_0, \underline{b}_1) \bmod 2$ and $\underline{a}_0 = \underline{b}_0$ imply $\underline{a}_1 = \underline{b}_1$. Hence $\underline{a} = \underline{b}$. ■.

Remark 3. Theorems 2 and 3 show that the binary sequence $\varphi(\underline{a}_0, \ldots, a_{e-1})$ contains all information of the original sequence $\underline{a}$. We guess that for any η, Theorem 3 is also correct.

REFERENCES

1. Z. D. Dai, Binary sequences derived from ML-sequences over rings I. Periods and minimal polynomials, *J. Cryptol.* **5,** No. 4 (1992), 193–207.
2. Z. D. Dai, T. Beth, and D. Gollman, Lower bounds for the linear complexity of sequences over residue rings, *in* "Advances in Cryptology—EUROCRYPT'90" (I. B. Damgard Ed.), Lecture Notes in Computer Science, Vol. 473, pp. 189–195, Springer-Verlag, Berlin, 1991.
3. M. Q. Huang, "Analysis and Cryptologic Evaluation of Primitive Sequences over an Integer Residue Ring," Doctoral dissertation of Graduate School of USTC, Academia Sinica, 1988.
4. M. Q. Huang and Z. D. Dai, Projective maps of linear recurring sequences with maximal p-adic periods, *Fibonacci Quart.* **30,** No. 2 (1992), 139–143.
5. V. L. Kurakin, The first coordinate sequence of a linear recurrence of maximal period over a Galois ring, *Discrete Math. Appl.* **4,** No. 2 (1994), 129–141.
6. A. S. Kuzmin and A. A. Nechaev, "A Construction of Noise Stable Codes using Linear Recurrences Over Galois Rings," Russian Mathematical Survey, Vol. 47, pp. 189–190, 1992.
7. A. S. Kuzmin and A. A. Nechaev, "Linear Recurring Sequences over Galois Rings," Russian Mathematical Survey, Vol. 48, pp. 171–172, 1993.
8. Qi Wenfeng, Yang Junhui, and Zhou Jinjun, ML-sequences over rings $Z/(2^e)$, *in* "Advances in Cryptology—ASIACRYPT'98," (K. Ohta and D. Pei, Eds.), Lecture Notes in Computer Science, Vol. 1514, pp. 315–325, Springer-Verlag, Berlin, Heidelberg, 1998.